



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/912,936	07/25/2001	Michael L. Wenocur	A-70554/RMA	7254

7590 01/04/2005

FLEHR HOHBACH TEST
ALBRITTON & HERBERT LLP
Suite 3400
Four Embarcadero Center
San Francisco, CA 94111-4187

EXAMINER

NGUYEN, MINH DIEU T

ART UNIT

PAPER NUMBER

2137

DATE MAILED: 01/04/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/912,936	WENOCUR ET AL.
	Examiner	Art Unit
	Minh Dieu Nguyen	2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 25 July 2001.
- 2a) This action is **FINAL**. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-54 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 1-15, 19-21, 23, 31-33, 36-38, 43-46, 48-49 and 54 is/are rejected.
- 7) Claim(s) 16-18, 22, 24-30, 34, 35, 39-42, 47 and 50-53 is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) All b) Some * c) None of:
1. Certified copies of the priority documents have been received.
2. Certified copies of the priority documents have been received in Application No. _____.
3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) Notice of References Cited (PTO-892)
- 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 1/8 & 2/12/02.
- 4) Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) Notice of Informal Patent Application (PTO-152)
- 6) Other: _____.

DETAILED ACTION

1. Claims 1-54 are pending.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claim 2 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

"the resource tag" in item B. lacks antecedent basis.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 1-9, 11-14, 23, 31, 43-46, 48-49 and 54 are rejected under 35 U.S.C. 103(a) as being unpatentable over Herz (6,460,036) in view of Kaufman (5,666,415).

- a) As to claims 1-2 and 54, Herz discloses a system and method for providing customized electronic newspapers and target advertisements comprising sending a first information item to a specified user (col. 34, lines 44-49); receiving, back

Art Unit: 2137

from the specified user, the first information sent earlier and a user second information item (col. 37, lines 65-66); verifying the user second information item (col. 38, lines 1-2) and granting access to the particular resource only if the first crypto transformation of the first information item has a predetermined relationship with the second crypto transformation of the second information item (col. 38, lines 19-23).

Herz discloses the server authenticates a user's pseudonym to grant access to the services, however he does not disclose compare a first crypto transformation of a first information item to a second crypto transformation of a second information item.

Kaufman discloses method and apparatus for cryptographic authentication comprising comparing a first crypto transformation of a first information item to a second crypto transformation of a second information item (Fig. 3, element 33).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of comparing a first crypto transformation of a first information item to a second crypto transformation of a second information item as Kaufman teaches in the system of Herz so as to provide an optimal authentication system (col. 1, lines 66-67).

- b) As to claim 3, Herz discloses the particular resource comprises an e-mail message (col. 6, lines 36-39).
- c) As to claim 4, Herz discloses the particular resource comprises a promotional coupon (col. 33, lines 54-55).
- d) As to claim 5, Herz discloses the particular resource comprises an information item in electronic form (col. 6, lines 9-12).

Art Unit: 2137

- e) As to claim 6, Herz discloses the particular resource comprises a storymail story (col. 6, lines 12-14).
- f) As to claim 7, Herz discloses the resource tag comprises a message tag or a coupon tag (col. 31, lines 64-67).
- g) As to claim 8, Herz discloses the resource tad is generated as the result of a reversible crypto transformation (col. 33, line 64 to col. 34, line 5).
- h) As to claim 9, Herz discloses the first information item comprises a redundancy field (col. 36, lines 48-50) and the second information item comprises a resource identifier field which reads on user credentials (col. 37, lines 65-66) and the transformation comprises a transformation of one or more of the redundancy field and the resource identifier field (col. 36, lines 48-51).
- i) As to claim 11, Kaufman discloses the transformation comprises a transformation of a redundancy field, a resource identifier field and other information (Fig. 3).
- j) As to claim 12, please see addressed claims 7-10.
- k) As to claim 13, Herz discloses the resource tag is sent by any one of conventional e-mail, story Enabled e-mail, display on a web page, or hardcopy media (col. 31, lines 64-67; Fig. 1).
- l) As to claim 14, Herz discloses the fields of a resource tad are based on one or more secret keys known to the resource owner (col. 37, lines 36-38).
- m) As to claim 23, Herz discloses the redundancy field however he does not disclose the redundancy field comprises a cryptographic hash.

Art Unit: 2137

Kaufman discloses a method of encrypting messages using hash functions (col. 2, lines 36-47).

n) As to claim 31, Kaufman discloses the verification of the user's credential is based on a challenge/response authentication protocol (col. 3, lines 1-3).

o) As to claims 43-46 and 48-49, Kaufman discloses the comparison comprises a logical operation wherein the logical operation performed on a bit, byte, multi-bit, multi-byte basis (Fig. 3).

6. Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over Herz (6,460,036) in view of Kaufman (5,666,415) and further in view of Jovicic et al. (5,855,007).

Herz and Kaufman do not disclose at least one of the redundancy field and resource identifier field include a message number.

Jovicic discloses an electronic coupon communication system for generating and redeeming unique product discount coupons over public computer networks wherein at least one of the redundancy field and resource identifier field include a message number include a message number (Fig. 3).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of having message number element in at least one of the redundancy field and resource identifier field as Jovicic teaches in the system of Herz and Kaufman so as to include more specific elements related to the information exchanged between clients and servers.

Art Unit: 2137

7. Claims 15, 19-21 and 32-33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Herz (6,460,036) in view of Kaufman (5,666,415) and further in view of Schneier (Applied cryptography).

a) As to claim 15, Herz and Kaufman do not disclose block encryption.

Schneier discloses cascading multiple block algorithms (page 367-368).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of cascading block enciphering as Schneier teaches in the system of Herz and Kaufman so as to strengthen transformation algorithm.

b) As to claims 19-21, Herz discloses the resource tad has an arbitrary length (col. 36, lines 45-50), however Herz and Kaufman do not disclose the crypto transformation is performed by a block cipher.

Schneier discloses block ciphers and cipher block chaining mode wherein the cipher block chaining mode operates with an initialization vector (page 190-194).

c) As to claim 32, Kaufman discloses public key cryptography (col. 2, lines 21-31). However, he does not disclose using public key in authentication.

Schneier discloses authentication using public key cryptography (page 53-54).

d) As to claim 33, Schneier discloses the private key comprises a RSA private key (page 466-469).

8. Claims 36-37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Herz (6,460,036) in view of Kaufman (5,666,415) and further in view of Schneier (5,956,404).

Art Unit: 2137

a) As to claim 36, Herz and Kaufman disclose the challenge-response protocol indicates that user communicating with server has current access to a secret key, however they do not disclose a secret key associated with a key identifier.

Schneier discloses a key ID bits identifying the private key (Abstract).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of having a key identifier associating with a private key as Schneier teaches in the system of Herz and Kaufman so as to better track the information (col. 2, lines 55-60).

b) As to claim 37, Schneier discloses the secret key comprises a triple-DES based secret key (col. 5, line 66 to col. 6, line 13).

9. Claim 38 is rejected under 35 U.S.C. 103(a) as being unpatentable over Herz (6,460,036) in view of Kaufman (5,666,415), in view of Schneier (5,956,404) and further in view of Thakkar et al. (6,260,142).

Herz, Kaufman and Schneier do not disclose the key identifier appears as one field of the user credential information.

Thakkar discloses method and apparatus for secure group communications wherein credentials may include key ID (col. 4, lines 20-22).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of having a key identifier associating with a private key as Schneier teaches in the system of Herz and Kaufman so as to better track the information.

Allowable Subject Matter

10. Claims 16-18, 22, 24-30, 34-35, 39-42, 47 and 50-53 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dieu Nguyen whose telephone number is 571-272-3873. The examiner can normally be reached on M-F 6:00-2:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on 571-272-3868. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

Minh Dieu Nguyen
Examiner
Art Unit 2137

mdn
mdn
12/17/04

Andrew Caldwell
Andrew Caldwell